

ABSTRACT

A system and method is presented for enciphering information using the Advanced Encryption Standard (AES) algorithm in which a subprocessor is configured to manipulate data as it is being loaded into the subprocessor memory. Thus, unlike implementations in the prior art, which require complete loading of data into a subsystem memory before data manipulation thereby creating a potential bottleneck in memory, this invention reduces the potential bottleneck in memory.